Section 1

INTRODUCTION

Contents

Purpose....1-1
Organization....1-1
General Considerations....1-2
Using the Topic-Specific Tools....1-2
Using the Tools in Each Inspection Phase....1-3
Performance Testing....1-4
Validation....1-5
Characterization of the Physical Security Systems Topic....1-5
Data-Collection Guidelines....1-7
Integrated Security Management....1-11

Purpose

The Physical Security Systems Inspectors Guide provides the inspector with a set of detailed tools and references that can be used to plan, conduct, and close out an inspection of physical security systems (PSSs). These tools serve to promote consistency, assure thoroughness, and enhance the quality of the inspection process.

The guide is intended to be useful for both novices and experienced inspectors. For the experienced inspector, information is organized to allow easy reference and to serve as a reminder when conducting inspection activities. For the novice inspector, the information can serve as a valuable training tool. With the assistance of an experienced inspector, the novice inspector should be able to use the tools and reference materials to collect and interpret data more efficiently and effectively.

Organization

This introductory section (Section 1) describes the inspection tools and outlines their use. Sections 2 through 9 provide detailed guidance for inspecting each major PSS subtopic:

- Section 2—Intrusion Detection and Assessment
- Section 3—Entry and Search Control
- Section 4—Badges, Passes, and Credentials
- Section 5—Barriers
- Section 6—Communications
- Section 7—Testing and Maintenance
- Section 8—Support Systems
- Section 9—Systems Management

Section 10 (Interfaces) contains guidelines to help inspectors coordinate their activities both within subtopics and with other topic teams. Information is provided on the integration process, which allows topic teams to align their efforts and benefit from the knowledge and experience of other topic teams. The section provides some of the common areas of interface for the PSS team, and explains how the integration effort greatly contributes to the quality and validity of inspection results.

Section 11 (Analyzing Data and Interpreting Results) contains guidelines on how to organize and analyze data collected during inspection activities. These guidelines include possible impacts of specific information on other topics or subtopics, and some experience-based information on the interpretation of potential deficiencies.

Appendices A through D provide procedures for testing the various systems and items of equipment that are commonly used in DOE facilities, with guidelines for evaluating test results. Appendix A (Intrusion-Detection Systems) includes performance tests for testing a variety of intrusion-detection systems:

- Exterior Perimeter Sensors
- Interior Sensors
- Perimeter Closed Circuit Television (CCTV) Systems
- Interior CCTV Systems
- Alarm Processing and Display.

Appendix B (Access Control Systems) contains tests related to the effectiveness of entry control and detection equipment.

Appendix C (Communications Equipment) contains performance tests on radio equipment and duress alarms.

Appendix D (Support Systems) addresses the testing of equipment associated with power sources and tamper protection.

Appendix E (Personnel and Procedures) provides guidelines for designing and conducting site-specific tests of personnel and procedures. Candidate procedures, sample scenarios, and an example test plan are included.

General Considerations

The guide contains tools and information that inspectors frequently need. It is designed as a reference manual, to be used at the discretion of the inspector; an inspector selects the tools that are most useful on an inspection-specific basis. Generally, the information is presented according to safeguards and security subtopics, so specific subjects are easy to locate. Although the guidelines cover a variety of inspection activities, they do not and cannot address all protection program variations and systems used at DOE facilities. The tools may have to be modified or adapted to meet inspection-specific needs, and inspectors may have to design new tools or activities to collect information not specifically covered in the guide.

The information in this guide does not repeat all of the detailed information in DOE orders. Rather, it is intended to complement the orders by providing practical guidance for planning, collecting, and analyzing inspection data. Inspectors should refer to this guide, as well as DOE orders and other guidance, at all stages of the inspection process.

One purpose in developing the inspectors guides was to provide a repository for the collective knowledge of Office of Safeguards and Security Evaluations' (OA-10) most experienced inspectors that can be enhanced and updated as inspection methods improve and inspection experience accumulates. Every attempt has been made to develop specific guidelines that offer maximum utility to both novice and experienced inspectors. In addition to guidelines for collecting information, guidelines are provided for prioritizing and selecting activities, then analyzing and interpreting results. These guidelines should be viewed as suggestions rather than requirements. The specific guidelines should be critically examined and interpreted in light of inspection-specific and site-specific factors.

Using the Topic-Specific Tools

Sections 2 through 9, organized around the PSS subtopics, provide topic-specific information intended to help the inspectors collect and analyze inspection data. Each subtopic section is further divided into the following standard format:

- References
- General Information
- Common Deficiencies/Potential Concerns
- Planning Activities
- Performance Tests (if applicable)
- Data-Collection Activities.

References

The references include DOE orders that apply to the subtopic. Other relevant documentation, such as Executive Orders, Site Safeguards and Security Plans (SSSPs), implementation memoranda, memoranda of agreement, procedural guides, and certain manuals may be found in the References section. These references are used as the basis for evaluating the inspected program and for assigning findings. It is useful to refer to the applicable order during interviews and tours to ensure that all relevant information is covered.

General Information

The General Information section defines the scope of the subtopic. It includes background information, guidelines, and commonly used terms to help inspectors focus on the unique features and problems associated with the subtopic. It identifies the different approaches that a facility might use to accomplish an objective and provides typical examples.

Common Deficiencies/ Potential Concerns

This section addresses common deficiencies and concerns that OA-10 has noted on previous inspections, along with a short discussion giving more detail. Information in this section is intended to help the inspector further focus inspection activities. By reviewing the list of common deficiencies and potential concerns before gathering data, inspectors can be alert for these elements at the inspected facility during interviews, tours, and other data-gathering activities. Also, where appropriate, general guidelines are provided to help the inspector identify site-specific factors that may indicate whether a particular deficiency is likely to be present.

Planning Activities

This section identifies activities normally conducted during inspection planning. If applicable, specific activities or information available to inspectors are identified for all planning phases. These planning activities include document reviews and interviews with the facility PSS managers. The detailed information in the Planning Activities section is intended to help ensure systematic data collection, and to ensure that critical elements are not overlooked. Typically, the thoroughness of the planning effort will have a direct impact on the success of the inspection.

Performance Tests

General guidelines are provided to help the inspector identify site-specific factors that may indicate which specific performance tests may be particularly important. The details relating to PSS performance tests are found in Appendices A through E.

Data-Collection Activities

This section identifies activities that inspectors may choose to perform during data collection. This information is intended to be reasonably comprehensive, although it cannot address every conceivable variation. Typically, these activities are organized by functional element or by the type of system used to provide protection. Activities include tours, interviews, observations, and performance tests.

Inspectors do not normally perform every activity on every inspection. The activities and performance tests to be accomplished are normally selected during the planning effort. The listed activities are those that are most often conducted, and reflect as much OA-10 data-collection experience and expertise as possible. The activities are identified by alphabetical letter for easy reference.

Using the Tools in Each Inspection Phase

The inspection tools are intended to be useful during all phases of the inspection, including planning, conduct, and closure. The following summarizes the use of the inspection tools at each phase:

In the planning phase, inspectors:

- Use the General Information section under each subtopic to characterize the program and focus the review.

- Perform the activities identified under Planning Activities to gather the information necessary to further characterize the program and focus the review.

- Review Common Deficiencies/Potential Concerns to determine whether any of the deficiencies are apparent, and to identify site-specific features that may indicate that more emphasis should be placed on selected activities.

- Assign specific tasks to individual inspectors (or small teams of inspectors) by selecting performance tests and specific items from the Data-Collection Activities section. The assignments should be made to optimize efficiency and to ensure that all high-priority activities are accomplished.

- Review the guidelines under Section 10 (Interfaces) of the guide, to be considered when assigning tasks to ensure that efforts are not duplicated.

- Prioritize and schedule data-collection activities to optimize efficiency and to ensure that high-priority activities are conducted early in the process. A careful prioritization of these activities provides the opportunity to determine whether the available personnel resources and inspection time periods are sufficient to adequately evaluate the inspected topic.

- Review the applicable policy supplements to ensure that they are current with all applicable policy revisions, updates, and clarifications.

In the conduct phase, inspectors:

- Use the detailed information in the Data-Collection Activities section to guide interviews and tours. Inspectors may choose to make notes directly on photocopies of the applicable sections.

- Review Common Deficiencies/Potential Concerns after completing each data-collection activity to determine whether any of the identified deficiencies are apparent at the facility. If so, inspectors should then determine whether subsequent activities should be reprioritized.

- Review Section 11 (Analyzing Data and Interpreting Results) after completing each data-collection activity to aid in evaluation and analysis of the data, and to determine whether additional data are needed to evaluate the program. If additional activities are needed, inspectors should then determine whether subsequent activities should be reprioritized.

In the closure phase, inspectors:

- Determine whether the facility is complying with all applicable requirements.

- Use the Analyzing Data and Interpreting Results section to help analyze the collected data and assess the impacts of identified deficiencies. This will aid inspectors in determining the significance of findings, if any, and in writing the inspection report.

Performance Testing

Appendices A through E provide a set of commonly used performance tests that may be used directly or modified to address site-specific conditions or procedures. Since performance testing is one of the most important data-collection activities used in evaluating PSSs, the information on testing is rather extensive. Performance tests applicable to each subtopic are referenced in the subtopic section.

Performance testing differs from other data-collection tools in several important ways. First, performance testing is the most labor- and time-intensive of all the data-collection activities. Second, performance testing places the greatest demands on the resources of the inspected site and requires the highest degree of coordination and planning. Third, performance testing offers the greatest potential for generating safety or security problems. In some cases, data can be gathered using simpler data-collection tools, and extensive performance tests are not necessary. Performance tests must be carefully planned and coordinated before arriving on site in order to ensure the most efficient use of time and resources. This planning and coordination process continues up to the moment the test is administered.

The tests performed by the PSS topic team may involve equipment, personnel, procedures, or any combination of these. The ideal performance test stresses the system under examination up to the established limits of the site-specific threat. It should simulate realistic conditions and provide conclusive evidence about the effectiveness of the security system.

Equipment performance testing is designed to determine whether equipment is functional, has adequate sensitivity, and will meet its design and performance objectives. It is not sufficient for a component to meet the manufacturer's standards if the component proves ineffective during testing.

Personnel performance tests are intended to determine whether procedures are effective, whether personnel know and follow procedures, and whether personnel and equipment interact effectively.

Performance tests must always be coordinated with appropriate facility personnel. Some performance tests require that personnel being tested remain unaware that a test is being conducted. Particular care must be exercised to ensure that these types of tests are well-coordinated and safety factors carefully considered.

Unfortunately, realistic conditions are frequently difficult to simulate due to safety concerns, time and resource constraints, and the heightened security posture that results whenever an inspection is under way.

Determining which PSS to test is usually based on information uncovered during document reviews, interviews, and data-collection activities. If this information leads the inspectors to think that a weakness may exist along a particular adversary path, or if the maintenance history of a system indicates a potential weakness, the systems identified with these weaknesses should be tested. When testing, it is important not to concentrate on one aspect or component of a system at the expense of the overall system. Also, it is usually not necessary to test all component parts of a system to determine whether the system is effective. For example, if several doors installed in the same barrier wall are equipped with an identical alarm system, testing a few doors rather than all doors is normally sufficient.

Validation

Validation is the procedure used to verify, with site representatives or points of contact, the accuracy of the information OA-10 inspectors have obtained during data collection. It is also particularly important that the site representatives or points of contact understand what is being validated. These procedures, discussed in the OA-10 Appraisal Guide, include on-the-spot validations, daily validations, and summary validations. On-the-spot validations verify the data at the time of collection. On-the-spot validations are particularly important during performance testing because there may be a number of people present and it is frequently difficult to reassemble these same people for the daily and summary validations. All on-the-spot validations should be validated during daily validations, which are normally conducted at the end of the day during the data-collection phase of the inspection. The summary validation is usually conducted at the end of the data-collection phase of the inspection. It is important for team members to keep track of the information covered in on-the-spot and daily validations so that it can be reiterated during the summary validation.

Characterization of the Physical Security Systems Topic

Physical security is defined as the use of intrusion detection and assessment, entry and search control, barriers, communications, testing and maintenance, and supporting systems and interfaces to deter, detect, annunciate, assess, delay, and communicate an unauthorized activity. A PSS is designed to employ a complementary combination of these components (see Figure 1), augmented by practices and procedures specific to each location.

All DOE security assets, both tangible and intangible, are protected from theft, diversion, sabotage, espionage, and compromise that might adversely affect national security, program continuity, the environment, or the health and safety of employees or the public. There are four basic asset groups:

- Special nuclear material (SNM) and vital equipment
- Classified information
- Unclassified sensitive information
- Property and unclassified facilities.

SNM is defined and categorized according to quantity, composition, and attractiveness to others. Each category of SNM requires specific protection measures during storage, transit, and use. Most of these measures are discussed in DOE Order 5632.1C, "Protection and Control of Safeguards and Security Interests," and DOE Manual 5632.1C-1, "Manual for Protection and Control of Safeguards and Security Interests."

Vital equipment is defined as "equipment, systems, or components whose failure or destruction would cause unacceptable interruption to a national security program or an unacceptable impact on the health and safety of the public." Operations offices are responsible for identifying the vital equipment located at facilities under their purview.

The level of protection afforded classified matter depends upon the level of classification or category assigned: Top Secret, Secret, or Confidential. Classified matter can be information, documents, parts, components, or other material.

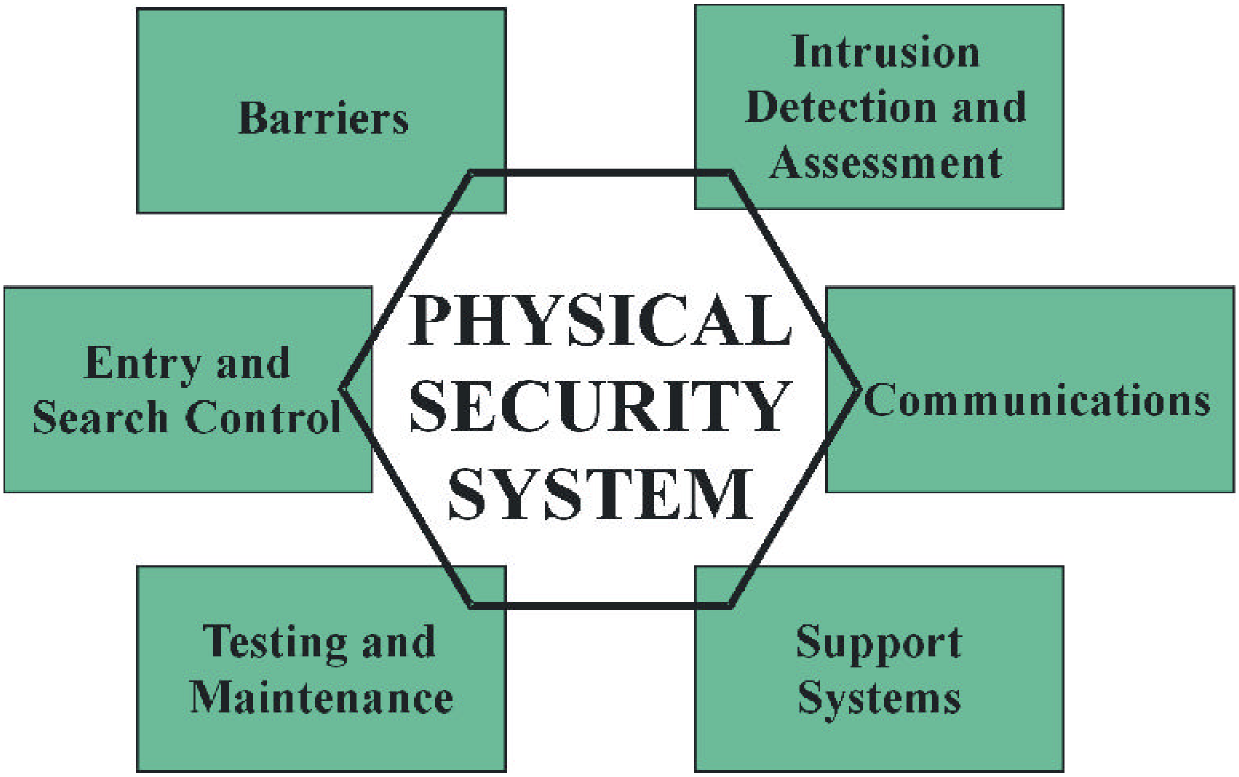


Figure 1. Physical Security System Components

Increased levels of protection are provided to high-consequence assets. The most significant protection efforts center on nuclear weapons and Category I SNM. Also, intrusion-detection systems and entry-control systems that protect classified communications centers and computer centers are of concern to the physical security topic.

The protection standards are specific to the type of security interest, as well as to specific targets. Consequently, there are various levels of sophistication used to protect different assets. The design of a PSS requires an engineering perspective, incorporating site-specific requirements determined by vulnerability assessments and resulting in a level of protection consistent with DOE guidance. Levels of protection for particular safeguards and security interests are provided in a graded fashion in accordance with the potential risks.

A PSS can be viewed as protection provided along an adversary penetration path where either force, deceit, or stealth tactics may be employed to defeat the system (see Figure 2, an example of layered protection of SNM). Force, deceit, and stealth are characterized as:

- **Force:** Adversary actions directed at overcoming elements of the physical protection system by overt aggressive activities, which the adversary expects to be detected and thus is prepared to forcefully defend against the response.

- **Deceit:** Adversary actions directed at overcoming elements of the physical protection system by normal submission to an element with the expectation that unauthorized conditions, such as a fake badge or shielded material, will not be detected.

- **Stealth:** Adversary actions directed at overcoming elements of the physical protection system by avoiding or deactivating these elements in an attempt to prevent detection.

One approach in determining whether assets are at risk is to identify the existing adversary paths leading into and out of the target area. This is perhaps best visualized by color coding a large site map and highlighting the layers of protection afforded the various assets. This process will identify the various components of a typical PSS (that is, barrier systems, entry-control systems, and interior and exterior intrusion-detection systems). A color-coded map will help the inspector visualize the overall methodology used by the site and allow evaluation of system weaknesses. Also, this will aid in the selection of performance tests. This characterization can be aided by using a series of tools.

The completed site map, marked to indicate the various layers of protection comprising the PSS should be compared with a verified listing of assets to ensure that all assets are afforded appropriate protection.

The inspector should then begin to identify and describe the component parts of the PSS.

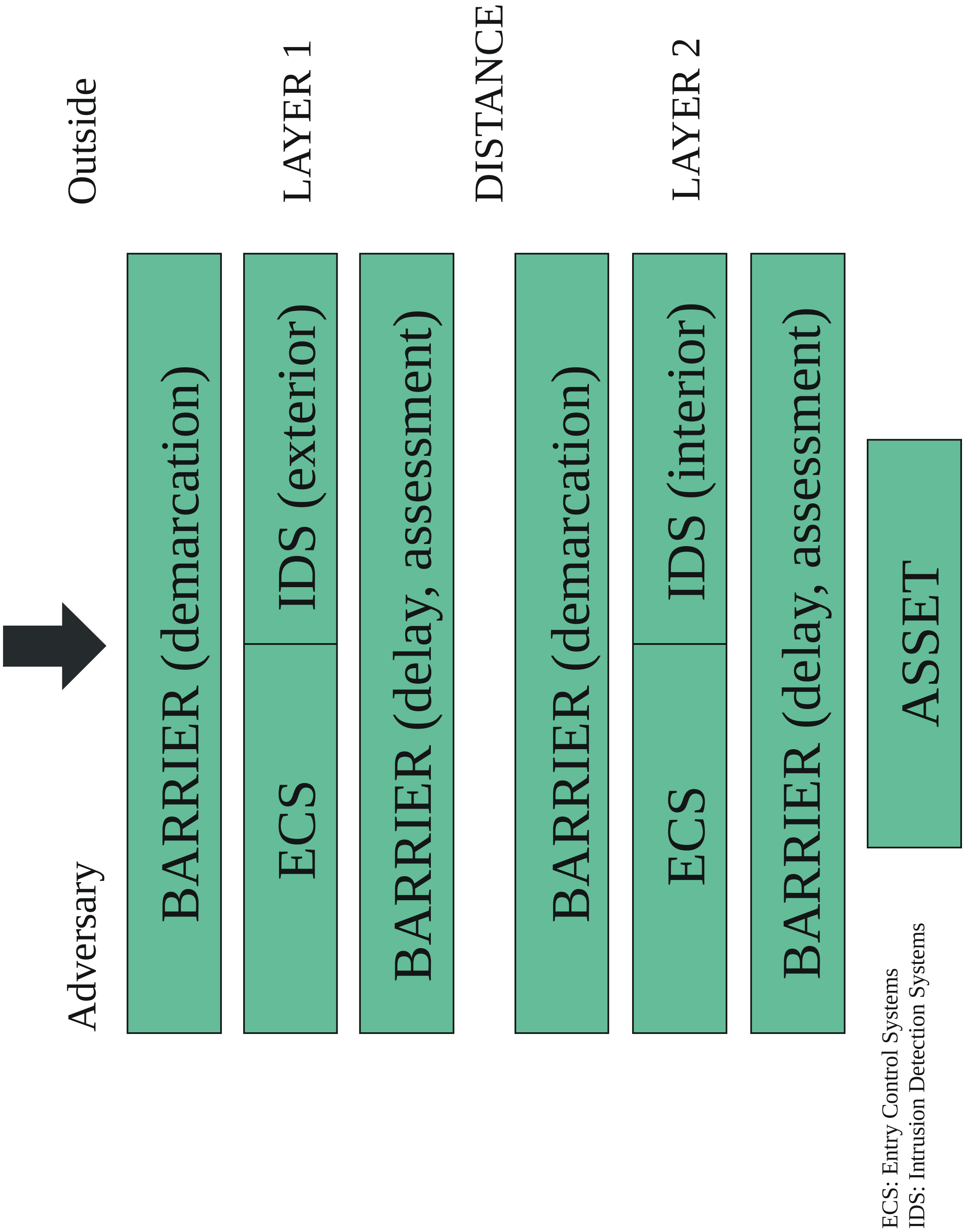
Data-Collection Guidelines

This section provides general data-collection guidelines for document reviews, interviews, and tours. More specific guidance is included in the individual subtopic sections.

An integral part of the inspection planning process involves collection, review, and analysis of data relative to the site. Site-specific assets and the protective methods used will provide insight on the site’s mission, operations, and processes.

The purpose of briefings presented by the operations office and contractor representative is to provide the PSS inspection team with a broad understanding of the site mission. Additional information can be obtained from a review of documents during the planning phase and from interviews with site representatives.

To focus the inspection process and ensure that inspection resources are expended appropriately, the PSS inspection team should compile a listing of site assets described in the SSSP, grouping them into appropriate categories. Assets should be confirmed with topic teams dealing with



ECS: Entry Control Systems
IDS: Intrusion Detection Systems

Figure 2. Schematic Adversary Path to an SNM Asset

material control and accountability and control of classified documents and materials. Inspectors can draw certain conclusions and inferences based on the consequence of loss of these assets and, in so doing can further focus inspection efforts.

Elements to cover include:

- Organization charts; SSSP; site security plans; security plans for temporary material access areas; decontamination and decommissioning plans; listing of waivers and exceptions; past operations office survey reports and OA-10 inspection reports; facility asset list; and maps showing security areas, buildings, security posts, vital equipment areas, and SNM storage areas.

- A review of vulnerability assessments. The assessments provide the facility's evaluation of all potential pathways leading from outside the security area into respective target areas and characterize those pathways in terms of the delay and detection accumulated by the adversary en route to the target. The overall delay for each pathway is calculated and compared to protective force response times to determine the protective force's probability of adversary interruption prior to target access. By reviewing these assessments inspectors better identify which systems the facility considers to be most essential to asset protection. The following are some considerations for review of vulnerability assessments:

  – Priority of site-specific threats

  – Identification of "worst-case" (lowest probability of detection and/or shortest amount of delay) pathways into a facility

  – Identification of systems (detection, assessment, delay) that are most critical in providing protection for DOE assets

  – Determination of the assumed detection probabilities for each system

  – Determination of the credit taken by the facility for assessment (immediate assessment vs. delayed assessment)

  – Identification of the last possible point that an adversary must be detected to allow adequate response/adversary interruption by the facility protective force

  – Graded protection and defense-in-depth

  – Comparison of vulnerabilities against findings and resolution of past OA-10 inspections and operations office surveys.

The review of key documents and selected records are two important inspection activities in the evaluation of PSS effectiveness. The document review begins during the planning phase with the review of the SSSP, survey and inspection reports, and other documents. Review of these documents reveals the physical protection philosophy and approach taken to implement the safeguards and security requirements mandated by DOE orders.

Information obtained from the document review will establish the inspection baseline for (1) verifying information received from briefings, tours, and interviews; (2) determining the site-specific threat; (3) identifying site/facility assets; (4) implementing PSS corrective actions; (5) establishing response posture and protection strategy; and (6) detailing standard operating procedures.

Records to be reviewed include: material control and accountability (MC&A) records; operations logs; test records; PSS maintenance, testing and repair records; trend analysis information; occurrence reports; force-on-force after-action reports; and other records identified during the course of the inspection.

Procedures to be reviewed include protective force post orders, maintenance procedures, MC&A procedures, and facility operating procedures.

The inspection team should review records and procedures to determine whether:

- Required PSS records are kept
- System tests are performed and documented as required
- System maintenance is performed as required
- PSS procedures are comprehensive and effective
- Anomaly resolution is timely and effective
- The overall protection afforded DOE assets has been considered

Typically, the inspection team begins its activities by meeting with the DOE operations office point of contact at the site to:

- Review follow-up items from planning activities
- Work out details of the inspection schedule (for example, specific points of contact for each activity)
- Discuss any issues that may have developed subsequent to planning activities.

The inspection team generally tours the facility as early as possible. More detailed tours of key areas are scheduled as needed.

Although inspectors are likely to examine facility drawings and analyze potential adversary paths, facility tours are essential to gain the level of understanding required by the inspection team. The purposes of these tours are to:

- Become familiar with the site and facility layout
- Observe the actual layout of the overall PSS and individual elements of the system
- Verify that the documentation previously examined accurately reflects the current condition and configuration of the site
- Ensure that the systems described in documentation are implemented and operational
- Identify anomalies or deficiencies that require further investigation
- Select specific areas or components as candidates for performance testing.

Tours provide the opportunity to place the PSS documentation and briefings into perspective, because the inspector witnesses the operating environment and can note the intangibles that affect systems design and operation. To obtain maximum benefit from the tour, the topic team should:

- Minimize unnecessary inconvenience to tour guides and facility operations and personnel
- Try to observe procedures during normal operations (e.g., observe vehicle search procedure while testing equipment at a post)
- Have the people who normally work in the area demonstrate the procedures rather than having a supervisor demonstrate how they think the procedure is performed
- Take notes on areas that may require further review (e.g., vault thickness, protection against penetrations into vaults)
- Ensure that tour logistics are carefully arranged.

During the initial tours, inspectors should verify:

- Locations and boundaries of material access areas (MAAs) and protected areas (PAs)
- Category designation of MAAs and PAs
- Locations of MAA and PA access portals
- Locations of normal transfer points and paths between MAAs
- Locations and types of security equipment installed

- Location of the alarm stations.

Additionally, inspectors should confirm:

- General quality and condition of the physical barriers
- Entry control procedures and methods employed at access portals (contraband detection equipment and procedures, badge checks, badge exchanges, card readers, and biometrics)
- Type of storage areas (vaults, vault-type rooms, alarmed rooms, safes, locked filing cabinets, or locked rooms)
- Location of emergency exits
- Types and approximate quantities of SNM in use or being processed.

The selection of limited scope performance tests is based largely on the analysis performed during the planning phase of the inspection and on information derived from interviews with operations office and contractor representatives. Typical test measures verify whether:

- PSSs are accurately characterized in vulnerability assessments and security plans
- Response times are consistent with those identified in security plans
- Equipment is tested and calibrated according to traceable specifications
- Procedures are complete and describe the actual methods of operation
- Personnel adhere to procedures in performing their activities
- Personnel are knowledgeable of their duties and responsibilities
- Equipment is in good repair.

Interviews clarify impressions and allow insight into facility operating procedures. Interviews with personnel at all organizational levels are recommended. Frequently, discussions with personnel involved in “hands on” operations will reveal whether policies and directives of management are effectively communicated and implemented, and whether the systems actually function as described in the documentation.
Personnel to consider interviewing include DOE and contractor security managers, facility managers and staff, vault/vault-type room custodians, Security Police Officers (SPOs), security technicians/specialists, physical security system maintenance personnel, systems engineers and programmers, and Central Alarm Station (CAS) and Secondary Alarm Station (SAS) operators. Other personnel may be interviewed as needed. Interviews are not necessarily formal, and often take the form of discussions during facility tours or performance testing.

Integrated Security Management

In the environment, safety, and health (ES&H) arena, DOE uses an approach called integrated safety management (ISM) that has helped to improve management of ES&H programs. As part of the ISM approach, DOE has delineated guiding principles and core functions of safety management that establish the framework for integrated safety management.

The seven ES&H guiding principles of ISM are:

- Line management responsibility
- Clear roles and responsibilities
- Competence commensurate with responsibilities
- Balanced priorities
- Identification of standards and requirements
- Hazard controls tailored to work being performed
- Operations authorization.

The five ES&H core functions of ISM are:

- Define work
- Analyze vulnerabilities
- Identify and implement controls
- Perform work within controls
- Feedback and improvement.

Several DOE sites are considering the benefits of adopting a similar approach for safeguards and security programs. This approach is generally referred to as integrated security management. Development of the safeguards and security policies, such as the integrated security management concept, is the responsibility of the Office of Security and Emergency Operations (SO). If adopted, integrated security management would be formally established through the DOE directives system.

Although not currently a formal policy in the security arena, many aspects of the guiding principles and core functions of DOE's ES&H ISM policy are fundamental to management of any program. In addition, it is sometimes useful to apply ISM concepts in planning and conducting safeguards and security inspections and in analyzing data related to the effectiveness of DOE site safeguards and security programs. Further, the use of ISM concepts can be a useful approach for diagnosing the root causes of identified weaknesses, and thus can benefit the site by organizing inspection results in a manner that highlights root causes.

In view of the potential benefits of integrated security management, OA has taken a proactive approach to designing this Physical Security Systems Inspectors Guide to reflect certain aspects of the integrated security management concept. Specifically, OA has organized the relevant section of the Physical Security Systems Inspectors Guide (i.e., Section 9, Systems Management) to parallel certain aspects of the ISM principles and core functions. Also, Section 11, Analyzing Data and Interpreting Results, includes a brief discussion of the use of the integrated security management concepts as an analytical tool.

For the purposes of this Physical Security Systems Inspectors Guide, OA has established four general categories that encompass the concepts embodied in the guiding principles and core functions of ISM. These four categories are listed in below:

Line Management Responsibility for Safeguards and Security. This category encompasses the corresponding ISM guiding principles that relate to management responsibilities (i.e., line management responsibility for safety, clear roles and responsibilities, and balanced priorities).

Personnel Competence and Training. The category encompasses the ISM guiding principle related to competence of personnel (i.e., competence commensurate with responsibilities). It also encompasses DOE requirements related to ensuring that personnel performing safeguards and security duties are properly trained and qualified, and the need for sufficient requirements and an appropriate skill mix.

Comprehensive Requirements. This category encompasses the corresponding ISM guiding principles and core functions that relate to policies, requirements, and implementation of requirements (i.e., identification of safeguards and security standards and requirements, protection measures tailored to security interests and programmatic activities, operations authorization, define work, analyze vulnerabilities, identify and implement controls, and perform work within controls).

Feedback and Improvement. This category encompasses the corresponding ISM core function (i.e., feedback and improvement) and DOE requirements related to DOE line management oversight and contractor self-assessments.

It is important to note that the categories above are only used to organize information in the inspectors guide in a way that will help inspectors gather data about management performance in a structured and consistent manner. OA will not use the guiding principles or core functions as a basis for the ratings, and will not cite them as the basis for findings (unless and until a formal policy is promulgated). Further, OA has only identified general categories of information that would be expected to be in an integrated security management program. OA has not attempted to specifically define guiding principles for the safeguards and security arena because the development of such policies is the responsibility and prerogative of SO.